

Studienordnung der Universität des Saarlandes für den Master-Studiengang Cybersecurity

Vom xxx

Die Fakultät für Mathematik und Informatik der Universität des Saarlandes hat auf Grund von § 60 Saarländisches Hochschulgesetz vom 30. November 2016 (Amtsbl. I S. 1080), zuletzt geändert durch Gesetz vom 10. April 2019 (Amtsbl. S. 412) und auf der Grundlage der Gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik) vom 2. Juli 2015 (Dienstbl. Nr. 72, S. 616), zuletzt geändert durch Ordnung zur Änderung der Gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik) vom 28. April 2016 (Dienstbl. Nr. 47, S. 404) folgende Studienordnung für den Master-Studiengang Cybersecurity erlassen, die nach Zustimmung des Senats der Universität des Saarlandes hiermit verkündet wird.

§ 1 Geltungsbereich

Diese Studienordnung regelt Inhalt und Aufbau des Master-Studiengangs Cybersecurity auf der Grundlage der Gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik) vom 2. Juli 2015 (Dienstbl. Nr. 72, S. 616), zuletzt geändert durch Ordnung zur Änderung der Gemeinsamen Prüfungsordnung für die Bachelor- und Master-Studiengänge der Fakultät 6 (Naturwissenschaftlich-Technische Fakultät I – Mathematik und Informatik) vom 28. April 2016 (Dienstbl. Nr. 47, S. 404) sowie der Fachspezifischen Bestimmungen für den Masterstudiengang Cybersecurity vom xxx 2021 (Dienstbl. Nr. xxx). Zuständig für die Organisation von Lehre, Studium und Prüfungen ist die Fakultät für Mathematik und Informatik.

§ 2 Ziele des Studiums und Berufsfeldbezug

Ziel dieses Master-Studiengangs ist es, auf eine anspruchsvolle nationale und internationale Forschungs- und Entwicklungstätigkeit im Bereich der Cybersecurity vorzubereiten. Der Master-Studiengang Cybersecurity zielt darauf ab, den Studierenden unterschiedliche und sich ergänzende Möglichkeiten zur Vertiefung des Themenfelds der Cybersicherheit zu bieten. Studierende können sich in den Bereichen der Kryptographie, Privatsphäre, Sicherheit von Software, Systemen und Netzwerken, formalen Methoden oder rechtlichen Aspekte der Cybersicherheit vertiefen, und dabei gleichzeitig gezielte verwandte Themenblöcke der Informatik erarbeiten. Der Abschluss ermöglicht einen direkten Einstieg in Cybersicherheitsforschung, und vermittelt gleichzeitig tiefes Wissen, um nicht-wissenschaftliche Tätigkeiten im Kontext der Cybersicherheit in der Privatwirtschaft oder im öffentlichen Bereich aufnehmen zu können.

§ 3 Studienbeginn und Studiendauer

(1) Das Studium kann jeweils zum Winter- und Sommersemester eines Jahres aufgenommen werden.

(2) Das Lehrangebot ist so organisiert, dass das Studium in vier Semestern abgeschlossen werden kann (Regelstudienzeit).

§ 4

Art der Lehrveranstaltungen

Das Lehrangebot wird durch Lehrveranstaltungen folgender Art vermittelt:

1. Vorlesungen (V, Regelgruppengröße = 100): Sie dienen zur Einführung in ein Fachgebiet und vermitteln u. a. einen Überblick über fachtypische theoretische Konzepte und Prinzipien, Methoden und Fertigkeiten, Technologien und praktische Realisierungen. Vorlesungen geben Hinweise auf weiterführende Literatur und eröffnen den Weg zur Vertiefung der Kenntnisse durch Übungen, Praktika und ergänzendes Selbststudium.
2. Übungen (Ü, Regelgruppengröße = 20): Sie finden überwiegend als Ergänzungsveranstaltungen zu Vorlesungen bevorzugt in kleineren Gruppen statt. Sie sollen den Studierenden durch Bearbeitung exemplarischer Probleme die Gelegenheit zur Anwendung und Vertiefung der in der Vorlesung vermittelten Lehrinhalte sowie zur Selbstkontrolle des Wissensstandes ggf. durch eigene Fragestellung geben.
3. Seminare (S, Regelgruppengröße = 15) erweitern die bereits erworbenen Kenntnisse und vermitteln durch das Studium von Fachliteratur und Quellen in Seminargesprächen, Referaten oder Seminararbeiten einen vertieften Einblick in einen Forschungsbereich. Sie dienen darüber hinaus dem Erlernen wissenschaftlicher Darstellungs- und Vortragstechniken sowie der Anleitung zu kritischer Sachdiskussion von Forschungsergebnissen. Zusätzlich können projektbezogene Arbeiten zu aktuellen wissenschaftlichen Diskussionen vorgesehen sein. Die dabei vertieften Inhalte können in einem Masterseminar die Grundlage für die Master-Arbeit bilden.
4. Praktika und Projekte (P, Regelgruppengröße = 15, Masterpraktikum, Regelgruppengröße = 6): In einem Praktikum oder Projekt werden fachpraktische Themen angeboten, die in die spezifische Arbeitsweise der betreffenden Studienfächer einführen. Die den Themen zugrundeliegenden theoretischen Kenntnisse erwirbt man durch Vorlesungen und Literaturstudien. Ein weiteres Ziel der Praktika ist die Vermittlung computergestützter Methoden durch praktische Anwendung. In Projekten werden in der Regel fachübergreifende Themen behandelt. Die Bearbeitung eines Themas bietet den Studierenden die Gelegenheit, in Gruppen unter Anleitung themenspezifische Aufgabenstellungen von der Konzeption bis hin zur praktischen Realisierung zu lösen. Man lernt hier einerseits die Zusammenhänge zwischen Theorie und Praxis durch eigene selbstständige Arbeit kennen, andererseits wird die Gruppenarbeit in Projekten gefördert. Die Teilnahme an Praktika oder Projekten kann vom Nachweis über die erfolgreiche Teilnahme an zugehörigen Vorlesungen und Übungen abhängig gemacht werden.

§ 5

Aufbau und Inhalt des Studiums

(1) Das Studium des Master-Studiengangs Cybersecurity umfasst eine Gesamtleistung von 120 Credit Points (CP) nach dem European Credit Transfer System (ECTS). Davon müssen mindestens 106 CP und maximal 110 CP als benotete Leistungen erbracht werden. Pro Semester sind in der Regel 30 CP zu erwerben.

(2) Das Studium umfasst Module zu folgenden Teilbereichen. Die Module und Modulelemente der einzelnen Teilbereiche, sowie jeweils die Art der Lehrveranstaltung, deren Semesterwochenstunden und Credit Points, Zyklus, sowie die Art der Prüfung und Benotung sind in Anhang A beschrieben.

1. 27 benotete Credit Points aus dem Bereich der Stammvorlesungen (je 9 CP, Wahlpflicht). Aus diesem Katalog sind verpflichtend die beiden Stammvorlesungen "Cryptography" und "Security" zu bestehen, sofern keine äquivalenten Vorleistungen aus einem vorangegangenen Studium nachgewiesen werden.

Studierende, welche die beiden Bachelor-Grundvorlesungen "Grundlagen der Cybersicherheit I" und "Grundlagen der Cybersicherheit II" in einem grundständigen Studium bereits bestanden haben, müssen die Stammvorlesung "Security" durch eine andere Stammvorlesung ersetzen.

2. Mindestens 30 und maximal 34 benotete Credit Points aus dem Bereich der Stammvorlesungen (je 9 CP), der Vertiefungsvorlesungen Cybersecurity (variable Anzahl an CP, zumeist jedoch 6 CP) oder der Seminare Cybersecurity (je 7 CP) (Wahlpflicht). Darin darf maximal ein weiteres Seminar (vgl. § 5 Absatz 2, Nr. 3) und eine weitere Stammvorlesung (vgl. § 5 Absatz 2, Nr. 1) enthalten sein.
4. 7 benotete Credit Points aus dem Bereich der Seminare Cybersecurity (je 7 CP, Wahlpflicht)
5. 12 benotete Credit Points des Master-Seminars (12 CP)
6. 30 benotete Credit Points der Master-Arbeit (30 CP)
7. Mindestens 14 unbenotete Credit Points ("freie Punkte") durch wählbare Module aus den Bereichen (Wahlpflichtbereich):
 - a. Masterpraktika (je 6 CP)
 - b. beliebig wählbare Module aus dem Bereich der Stammvorlesungen, Vertiefungsvorlesungen Cybersecurity oder Seminare Cybersecurity oder der entsprechenden Modulkategorien des Master-Studiengangs Informatik
 - c. Betreuung von Übungsgruppen (Tutorientätigkeit); in der Regel je 4 CP, wobei eine mehrfache Erbringung dieser Leistungen möglich ist, sofern die Übungsgruppen unterschiedlichen Modulen angehören.
 - d. Sprachkurse (maximal 6 CP; lebende Sprachen; nicht die Muttersprache)
 - e. Soft Skill Seminar
 - f. Industrie-Praktikum (maximal 6 CP), das auf Antrag an den Prüfungsausschuss genehmigt wurde.
 - g. Module, die auf Antrag an den Prüfungsausschuss genehmigt wurden. Studierende haben beispielsweise die Möglichkeit, einen Antrag an den Prüfungsausschuss auf Anerkennung des geleisteten studentischen Engagements (insbesondere Mitarbeit bei der akademischen Selbstverwaltung) sowie Veranstaltungen zu Schlüsselqualifikationen im Umfang von jeweils maximal 3 CP zu stellen.

(3) Im Wahlpflichtbereich können gesamte Module oder einzelne Lehrveranstaltungen belegt werden. Prüfungsleistungen, die bereits in die Bachelor-Prüfung eingegangen sind, können prinzipiell nicht in die Master-Prüfung eingebracht werden. Prüfungsleistungen aus dem Bachelor-Studium, die nicht in der Bachelor-Prüfung berücksichtigt wurden und einen Gesamtumfang von 30 CP nicht überschreiten, können in die Master-Prüfung eingebracht werden.

(4) Im Pflichtbereich werden insgesamt 42 CP erworben (30 CP davon entfallen auf das Modul "Master-Arbeit" und 12 CP auf das Modul "Master-Seminar") und im Wahlpflichtbereich sind mindestens 78 CP zu erwerben.

(5) Bei Veranstaltungen aus den Bereichen "Praktikum", "Seminar" sowie "Tutor", "Soft Skill Seminar" und "Sprachkurse" aus dem Wahlpflichtbereich stehen begrenzte Teilnehmerplätze,

abhängig von der entsprechenden Veranstaltung zur Verfügung. Die Zulassung wird durch den Modulverantwortlichen geregelt.

(6) Eine Prüfungsleistung ist entweder benotet oder unbenotet einzubringen. Die Teilung einer benoteten Prüfungsleistung in unbenotete und benotete Credit Points ist nicht möglich.

(7) Eine bestandene Prüfungsleistung der Stammvorlesungen Cybersecurity und Informatik kann in der Regelstudienzeit einmalig zur Notenverbesserung im gleichen Prüfungszeitraum (vgl. § 13 Abs. 4 der Prüfungsordnung) wiederholt werden. Bestandene Prüfungsleistungen der Vertiefungsvorlesungen Cybersecurity können einmalig zur Notenverbesserung im gleichen Prüfungszeitraum wiederholt werden, falls der Dozent zu Beginn der Veranstaltung die jeweilige Prüfungsleistung als verbesserbar ausweist. Dabei zählt das bessere Ergebnis. Ansonsten ist die Wiederholung einer bestandenen Prüfungsleistung nicht zulässig.

(8) Die Module der Stammvorlesungen im Wahlpflichtbereich werden mindestens einmal alle zwei Jahre angeboten. Seminare und Vertiefungsvorlesungen können einmalig angeboten werden. Der Studiendekan/Die Studiendekanin stellt in jedem Studienjahr ein hinreichendes Angebot sicher.

(9) Die Unterrichtssprache ist in der Regel Englisch und wird zu Beginn der Veranstaltung bekannt gegeben. Es wird gewährleistet, dass das Studium auch mit ausschließlich englischsprachigen Veranstaltungen erfolgreich abgeschlossen werden kann.

(10) Das Studienangebot in den verschiedenen Wahlpflichtbereichen kann modifiziert werden, wobei Änderungen vom Prüfungsausschuss zu genehmigen sind. Neue bzw. modifizierte Veranstaltungen, ihr Gewicht in CP und ihre Zugehörigkeit zu den Modulbereichen werden jeweils vor Semesterbeginn bekannt gegeben.

(11) Detaillierte Informationen zu den Inhalten der Module und Modulelemente werden im Modulhandbuch beschrieben, das in geeigneter Form bekannt gegeben wird. Änderungen an den Festlegungen des Modulhandbuchs, die nicht in dieser Studienordnung geregelt sind, sind dem zuständigen Studiendekan/der zuständigen Studiendekanin anzuzeigen und in geeigneter Form zu dokumentieren.

(12) Für Seminare und Praktika kann eine Anwesenheitspflicht bestehen, die der Dozent/die Dozentin zu Beginn des Moduls/Modulelements bekannt gibt. Die Pflicht der Anwesenheit ist erfüllt, wenn i.d.R. mindestens 85 % des zeitlichen Umfangs der Veranstaltung wahrgenommen wurde. Bei Fehlen aus triftigen Gründen können den Studierenden Ersatzleistungen angeboten werden.

(13) Inhaltsgleiche Module, die lediglich in verschiedenen Sprachen angeboten werden, gelten als ein Modul hinsichtlich der Anzahl der Prüfungsversuche sowie der Regelungen des Freiversuchs bzw. der Notenverbesserung, falls die Studienordnung diese vorsieht.

§ 6 Studienplan

Der Studiendekan/die Studiendekanin erstellt auf der Grundlage dieser Studienordnung einen Studienplan, der nähere Angaben über Art und Umfang der Modulelemente (Anhang A) enthält sowie Empfehlungen für einen zweckmäßigen Aufbau des Studiums gibt (Anhang B). Dieser wird in geeigneter Form bekannt gegeben. Das jeweils aktuelle Angebot in den verschiedenen Modulkategorien wird im Vorlesungsverzeichnis des jeweiligen Semesters bekannt gegeben.

§ 7 Studienberatung

(1) Die Zentrale Studienberatung der Universität des Saarlandes berät Interessierte und Studierende über Inhalt, Aufbau und Anforderungen eines Studiums. Darüber hinaus gibt es Beratungsangebote bei Entscheidungsproblemen, bei Fragen der Studienplanung und Studienorganisation.

(2) Fragen zu Studienanforderungen und Zulassungsvoraussetzungen, zur Studienplanung und -organisation beantwortet der Fachstudienberater/die Fachstudienberaterin für den Master-Studiengang Cybersecurity.

(3) Für spezifische Rückfragen zu einzelnen Modulen stehen die Modulverantwortlichen zur Verfügung.

§ 8 Auslandsaufenthalt

Es besteht die Möglichkeit, ein Auslandsstudium zu absolvieren. Die Studierenden sollten an einer Beratung zur Durchführung des Auslandsstudiums teilnehmen, ggf. vorbereitende Sprachkurse belegen und im Vorfeld über ein Learning Agreement die Anerkennung von Studienleistungen gemäß der einschlägigen Prüfungsordnung klären. Über Studienmöglichkeiten, Austauschprogramme, Stipendien und Formalitäten informieren sowohl das International Office als auch die Fachvertreter des entsprechenden Schwerpunktfachs. Aufgrund langer Antragsfristen und Bearbeitungszeiten bei ausländischen Universitäten wie Stipendiengebern sollte die Anmeldung für ein Auslandsstudium in der Regel ein Jahr vor Antritt des Auslandsaufenthalts im Prüfungssekretariat erfolgen.

§ 9 Master-Arbeit und Master-Seminar

(1) Durch die Anfertigung einer Master-Arbeit soll der/die Studierende nachweisen, dass er/sie Aufgabenstellungen aus den Bereichen der Cybersicherheit eigenständig bearbeiten kann. Die Arbeit entstammt einem der genannten Teilgebiete und wird individuell von einem Lehrenden des Master-Studiengangs Cybersecurity betreut. Die Bearbeitungszeit beträgt sechs Monate. Der mit der Master-Arbeit verbundene Aufwand wird mit 30 CP kreditiert.

(2) Jeder Studierende muss vor Abschluss der Master-Arbeit erfolgreich ein Master-Seminar mit direktem Bezug zum Thema der Master-Arbeit abgeschlossen haben. Dieses beinhaltet sowohl einen Vortrag über die geplante Themenstellung als auch eine schriftliche Beschreibung der geplanten Aufgabenstellung der Master-Arbeit.

(3) Die Master-Arbeit muss spätestens ein Semester nach erfolgreicher Teilnahme am Master-Seminar beim Prüfungssekretariat angemeldet werden. Nach Ablauf dieser Frist muss erneut ein Master-Seminar erfolgreich absolviert werden.

§ 11 In-Kraft-Treten

Diese Ordnung tritt zum xxx.2021 in Kraft.

Saarbrücken, xxx

Der Universitätspräsident
Univ.-Prof. Dr. Manfred J. Schmitt